Cyber Security Awareness Month Presentation
Information Security: In the Workplace

Welcome (Slide 1)
Welcome to a short information security lesson, "Information Security: In the Workplace." This tutorial is brought to you by the State of Tennessee's Security Management Group to promote Cyber Security Awareness Month.

Lesson Introduction (Slide 2)
This lesson will have five sections: anti-virus, pop-ups, SPAM filter, passwords and workplace awareness. At the end of the lesson there is a resource page incase you would like additional information.

Section One: Anti-Virus (Slide 3)
Computer viruses come from different sources, and can do harm to your computer. They could be on an e-mail attachment you receive, a file transferred from a flash-drive inserted into your computer, or you could get one from the Internet. In order to protect your computer from viruses your system administrator has installed anti-virus software on your computer. The anti-virus software should be set to run automatic scans and it can detect a virus you might receive between the scheduled scans. These scans run behind the scenes, so to speak, because they do not interrupt you as you work.

In the event that your anti-virus software catches a virus it will usually eliminate the virus right away, and you will not even know it happened. However, in some cases your anti-virus software might send you an alert telling you it was unable to destroy the virus. In that case you should contact your help desk as soon as possible so that a system administrator can assist you in removing the virus.

Section Two: Pop-Up Windows (Slide 4)
Have you ever been browsing the Internet and you get an annoying pop-up window that is an advertisement, or one that asks you to scan your machine for viruses? In some cases these pop-up windows can redirect you to a malicious site, or if you click on the message it can download malicious software to your computer. Instead of clicking on these messages you should close the pop-up window by clicking on the small "close" button at the top of the window.

Some browsers allow you to enable a pop-up blocker that will allow you to decide if you want to allow a pop-up or not. You will get a message at the top of your browser asking if you want to allow the pop-ups or not for that site. Use caution and only allow this function if you know that you are on a safe site.

Section Three: SPAM Filter (Slide 5)
Have you ever received e-mail from an unknown sender containing advertisements or notifying you that you just won $200,000? These e-mails are called SPAM or junk e-mails. Most of the SPAM e-mails are caught by a filter the State has installed on its e-mail system. The filter catches the e-mail as it is coming into the State's e-mail system and then it is quarantined. The State's e-mail system then sends an e-mail telling the recipient that it has quarantined an e-mail, and it provides information about the e-mail: the sender's name, sender's e-mail address and the subject of the e-mail. On occasion the SPAM filter will catch e-mail that is valid, and in that case you have the opportunity to release the e-mail from quarantine. However, you only want to release the e-mail if you are sure you know the person that sent the e-mail because some SPAM e-mail contains viruses or have malicious links that take you to a malicious website. If you determine the e-mail is indeed SPAM just delete the e-mail notice you received, do not release the e-mail from quarantine and try to delete the original e-mail.

Section Four: Passwords (Slide 6)
In the cyber or "computer" world passwords are like keys because along with your User ID they grant you access to systems like your computer, files stored on a server, and applications you use to do your job. Also, when you access your computer, files or applications the systems log your access. That is one of the reasons you do not want to share your login credentials with anyone. If someone were to use your login information to do things that are illegal or that damage the State's network it would be hard to prove it was not you that did the malicious deeds.

You should use hard to guess passwords. Your passwords should be at least 8 characters long, and they should include numbers and special characters. It is never a good idea to use the names of your family members, pets or favorite sports teams because those things are easily guessed by those who know you. Finally, dictionary words in any language are bad passwords because tools called "password crackers" can be used against your account to guess your password. These password crackers try all the words in the dictionary, and they do not stop at English words.

Have you ever wondered why you have to change your passwords every 90 days? The primary reason for this is that it is a preventative measure to avoid unauthorized access to the systems you use. Unknown to you, it is possible that someone could guess your password or obtain it some how without your consent. By changing your password more frequently you make it more difficult for someone to use your login credentials to gain unauthorized access to the systems you use.

Section Five: Workplace Awareness (Slide 7)
Take a moment to stop and consider the kind of information you work with on a regular basis. Is the information sensitive and/or confidential in nature? Do you know your policies for disposing of such information? Should the information be locked up before you leave your desk? Who is authorized to see the information you handle? If the information you handle is sensitive and/or confidential you should be a good custodian of the information and protect it as if it were your own.

When you leave your desk you should engage your screensavers and keyboard locks to protect the information on you computer. You lock your compute by pressing Ctrl + Alt + Delete at the same time and a window will come up giving you the option to lock your workstation. Press enter to lock your computer. Or you can simply press the Window and L keys at the same time to lock your workstation.

You should report an incident if you think someone has gained access to your computer without permission. You should report any suspicious behaviors of employees or visitors. And finally, you should report any incidents of unauthorized access in your workplace environment. Contact your supervisor if you are unsure how to report an incident.

Conclusion (Slide 8)
Thank you for taking the time to learn about information security in the workplace. For additional information please read the State of Tennessee Enterprise Information Security Policies. The Security Hotline can be used to report unauthorized access or a loss of confidential information.